УТВЕРЖДАЮ
Представитель
войсковой части 74455

«   »   2019 г.

УТВЕРЖДАЮ
Главный конструктор ОКР
«Скань-ФУ»
[redacted]
«   »   2019 г.

СОГЛАСОВАНО
Главный конструктор
СЧ ОКР «Скань-В»
[redacted]
«   »   2019 г.

СОГЛАСОВАНО
Главный конструктор
СЧ ОКР «Скань-18»
[redacted]
«   »   2019 г.

ПРОТОКОЛ

описания формата данных,

передаваемых из ПАК ПСАП

Настоящий протокол описывает формат данных, передаваемых из подсистемы сканирования в подсистему обработки ПАК ПСАП и из ПАК ПСАП в АПК «Скань-АС», и соответствие типов сущностей и полей для базы данных ООО «НТЦ «Вулкан».

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Тип сущности – тип, описывающий объект базы данных ООО «НТЦ «Вулкан» и АПК «Скань-АС». Тип сущности задается идентификатором entityTypeId и определяет структуру и поля объекта.

Поле типа сущности – имя поля в описании типа сущности.

Объект-сущность – объект базы данных ООО «НТЦ «Вулкан» или АПК «Скань-АС», структура и состав полей которого определяется типом сущности.

JSON-объект – объект-сущность, представленный в виде строки в формате JSON.

2 ФОРМАТ ДАННЫХ, ПЕРЕДАВАЕМЫХ ИЗ ПОДСИСТЕМЫ СКАНИРОВАНИЯ В ПОДСИСТЕМУ ОБРАБОТКИ ПАК ПСАП

Извлекаемые данные из подсистемы сканирования в подсистему обработки ПАК ПСАП передаются в порядке, описанном в «Протоколе интерфейса взаимодействия» данных подсистем. Они включают себя отчеты сканеров ИКС и результаты обработки файлов, перечень которых определен в ТЗ.

Извлекаемые данные передаются в виде массива JSON-объектов в поле «data» по команде запроса данных GetResult.

Соответствие типов сущностей и их полей, передаваемых из подсистемы сканирования для базы данных ООО «НТЦ «Вулкан», приведено в таблицах 1 и 2.

3 ФОРМАТ ДАННЫХ, ПЕРЕДАВАЕМЫХ ИЗ КОНТУРА ВЕБ-АГРЕГАЦИИ ПАК ПСАП В АПК «СКАНЬ-АС»

Данные из контура веб-агрегации ПАК ПСАП в АПК «Скань-АС» передаются в виде ZIP-архивов с текстовыми файлами, в которых каждая строка содержит JSON-объект.

. Они включают в себя результаты обработки файлов, загружаемых из веб-ресурсов, перечень которых определен ТЗ.

Соответствие типов сущностей и их полей, передаваемых из контура веб-агрегации ПАК ПСАП в АПК «Скань-АС», приведено в таблице 3.

4 ПОРЯДОК СОЗДАНИЯ ОБЪЕКТОВ-СУЩНОСТЕЙ

В таблицах 1–3 указаны типы сущностей и их поля, значения которых заполняются в результате обработки извлекаемых данных в ПАК ПСАП.

Данные, которые не соответствуют ни одному из типов сущностей базы данных ООО «НТЦ «Вулкан» или их полей, передаются в тех же JSON-объектах в формате, описанном в «Протоколе описания источников для сканирования и извлекаемых данных» и «Протоколе описания типов сканеров, форматов извлекаемых данных и типов файлов» ПАК ПСАП.

Кроме полей, указанных в таблицах 1–3, в ПАК ПСАП в каждом объекте-сущности указываются значения следующих полей:

– **id** – идентификатор объекта (GUID);
– **entityTypeId** – идентификатор типа сущности:
    a. 3 – subnet,
    b. 4 – host,
    c. 5 – port,
    d. 6 – credo,
    e. 7 – organization,
    f. 8 – department,
    g. 9 – personal,
    h. 12 – hostinterface,

~~i. ?? – account,~~

~~j. ?? – device_type,~~

~~k. ?? – os,~~

~~l. ?? – cve~~);

– **timeStamp** – отметка времени извлечения данных в формате UTC.

Поля типов сущностей, передаваемые в JSON-объектах и не входящие в структуру типов сущностей, переносятся в поле «extras» в подсистеме обработки ПАК ПСАП и в АПК «Скань-АС».

Для сохранения иерархической структуры передаваемых JSON-объектов используются объекты с типом сущности «relation», определяющие связи между объектами (значение поля «typeId» равно 1).

Таблица 1 – Соответствие типов сущностей и полей отчетов сканеров

Название сканера	Поле по протоколу описания типов и форматов сканеров и файлов	Тип сущности	Соответствующе е поле типа сущности
Nmap	host.address.addr	host	name
	host.hostnames.hostname.-name		domain
	host.ports		ports
	host.ports.port.portid	host.port	name
	host.ports.port.protocol		description
	host.ports.port.service.ostype	host.port.os	name
	host.ports.port.service.ostype		version
	host.os.os.osclass.osfamily	host.os	name
	host.os.os.osclass.osgen		version
	host.os.os.osclass.cpe		description
NNM	Report.ReportItem.port	port	name
	Report.ReportItem.protocol		description
	Report.ReportItem.cve	cve	name
АКИ и ПРУ	IpPu	host	name
	NetName		domain
	Latitude	host, organization	latitude
	Longitude		longitude
	Organization	organization	name
	Country, City, Address		address

Таблица 2 – Соответствие типов сущностей и полей результатов обработки файлов

Тип файла	Поле по протоколу описания типов и форматов сканеров и файлов	Тип сущности	Соответствующее поле типа сущности
Конфигурация оборудования Cisco	interface.interface_id	port	name
	interface.channel_number		number
	intgerface.description		description
	interface.ip_address	hostinterface	ip
	hostname	host	name
	username	credo	login
	password		password
	privilege		description
	ip_dhcp_pool.name	router	name
	ip_dhcp_pool.network.ip_address		localIp
	ip_dhcp_pool.network.mask		localMask
	ip_dhcp_pool. domain-name		description
	ip_dhcp_pool.dns-server		dns
	ip_domain.name	host	domain
	ip.name-server		name
	ip_ftp.username	credo	login
	ip_ftp.password		password
Файлы электронной почты	From, Sender, ReplyTo, To, Cc, Bcc, ResentFrom, ResentSender, ResentTo, ResentCc, ResentBcc	organization.personal	fio
	From, Sender, ReplyTo, To, Cc, Bcc, ResentFrom, ResentSender, ResentTo, ResentCc, ResentBcc	organization.personal.account	name, type="Email"
	DeliveredTo		name, type="Email"
	AuthenticationInfo		name, type="AuthenticationInfo"
База данных электронной почты	Contacts.CompanyName	organization	name
	Contacts.BusinessAddress, BusinessAddressCity, BusinessAddressCountry, BusinessAddressPostalCode, BusinessAddressPostOfficeBox, BusinessAddressState, BusinessAddressStreet, OfficeLocation		address
	Contacts.BusinessFaxNumber, BusinessTelephoneNumber		contacts
	Contacts.Department	organization.department	name
	Contacts.DisplayName, FirstName, FullName, Initials, LastFirstAndSuffix, LastName, MiddleName, Suffix	organization.personal	fio
	Contacts.CallbackTelepho-	organization.per-	name,

Тип файла	Поле по протоколу описания типов и форматов сканеров и файлов	Тип сущности	Соответствующе е поле типа сущности
	neNumber, CarTelepho-neNumber, Home2Telepho-neNumber, HomeFaxNumber, HomeTelephoneNumber, Mo-bileTelephoneNumber, Oth-erTelephoneNumber, Primary-TelephoneNumber, RadioTele-phoneNumber	sonal.account	type=”Phone”
	Contacts.EmailAddress		name, type=”Email”
	Contacts.HomeAddress, HomeAddressCity, HomeAd-dressCountry, HomeAddress-PostalCode, HomeAddress-PostOfficeBox, HomeAd-dressState, HomeAd-dressStreet, MailingAddress, OtherAddress, OtherAddress-City, OtherAddressCountry, OtherAddressPostalCode, OtherAddressPostOfficeBox, OtherAddressState, OtherAd-dressStreet		name, type=”Ad-dress”
	Contacts.JobTitle, Profession		name, type=”Job”
	Contacts.Language		name, type=”Lan-guage”
	Contacts.Birthday		name, type=”Birthday”
	Contacts.Account		name, type=”Ac-count”
	Contacts.NickName		name, type=”Nick-Name”
	Contacts.BusinessHomePage, PersonalHomePage		name, type=”Page”
	Contacts.ComputerNetwork-Name		name, type=”Computer-NetworkName”
	Contacts.Spouse		name, type=”Spouse”
	Contacts.ManagerName		name, type=”Manager-Name”
	Contacts.AssistantName		name, type=”As-sistantName”
	Contacts.AssistantTelepho-neNumber		name, type=”As-sistantTelepho-neNumber”

Тип файла	Поле по протоколу описания типов и форматов сканеров и файлов	Тип сущности	Соответствующее поле типа сущности
PCap	Messages.Message.IPv4.IpSrc, Messages.Message.IPv4.IpDst,	host	name
	Messages.Message.TCP.Port-Src, Messages.Message.TCP.-PortDst, Messages.Mes-sage.UDP.PortSrc, Mes-sages.Message.UDP.PortDst	host.port	name
	Messages.Message.Ethernet, Messages.Message.Ethernet16, Messages.Message.Ethernet32, Messages.Message.BridgedE-thernet	host.hostinterface	mac

Таблица 3 – Соответствие типов сущностей и полей результатов обработки данных из веб-ресурсов

Название веб-ресурса	Поле по протоколу описания источников для сканирования и извлекаемых данных	Тип сущности	Соответствующее поле типа сущности
cve.mitre.org	Name	cve	name
	Description		descr
nvd.nist.gov	CVE_Items.cve.CVE_data_meta.ID	cve	name
	CVE_Items.publishedDate		published-date-time
	CVE_Items.lastModifiedDate		last-modified-datetime
	CVE_Items.cve.problemtype.prob-lemtype_data.description.value		descr
	CVE_Items.configurations.n-odes.cpe_match.cpe23Uri		vulnerable-software-list
scans.io	hannobock.result	host	name
	hannobock.result, hannobock.name		domain
	noncedisrespect.ip, sniproxyscans.-target, sniproxyscans.host, polito-harcrawl.serverIPAdress		name
	noncedisrespect.ports	host.port	name
	politoharcrawl.url	host	domain

Название веб-ресурса	Поле по протоколу описания источников для сканирования и извлекаемых данных	Тип сущности	Соответствующее поле типа сущности
	project25499.host		name
	rapid7.ssl.endpoints.ip, rapid7.rdns.name, rapid7.fdns.value, rapid7.http.ip, rapid7.moressl.endpoints.ip, rapid7.cowrie, rapid7.nationalexposure.syn.value, rapid7.nationalexposure.nei.saddr, rapid7.nationalexposure.nei.daddr, rapid7.cio.ip, rapid7.https.ip, rapid7.tcp.saddr, rapid7.tcp.daddr, rapid7.udp.saddr, rapid7.udp.daddr		name
	rapid7.ssl.names.name, rapid7.rdns.value, rapid7.fdns.name, rapid7.moressl.names.name		domain
	rapid7.cio.banner.geo.loc		latitude
	rapid7.cio.banner.geo.loc		longtitude
	rapid7.ssl.endpoints.port, rapid7.http.port, rapid7.nationalexposure.syn.name, rapid7.nationalexposure.nei.sport, rapid7.nationalexposure.nei.dport, rapid7.cio.port, rapid7.https.port, rapid7.tcp.sport, rapid7.tcp.dport, rapid7.udp.sport	host.port	name
	rapid7.https.subject.o	host.organization	name
	rapid7.https.subject.c, rapid7.https.subject.st, rapid7.https.subject.l		address
	sba_email.target.ip	host	name
	sba_email.target.port	host.port	name
	tangled.remoteIPAddress	host	name
	tangled.domain		domain

Название веб-ресурса	Поле по протоколу описания источников для сканирования и извлекаемых данных	Тип сущности	Соответствующее поле типа сущности
	tangled.remotePort	host.port	name
	umichsandy.saddr, umichsandy.-daddr, umichhttps.source, umich-https.destination, umichcrypto.ip, umichheartbleed.host	host	name
	umichcrypto.domain		domain
	umichsandy.sport, umichsandy.d-port, umichhttps.destinationport, umichhttps.sourceport	host.port	name
	ecrimelabs.victim, ecrimelabs.sol-dier	host	name
	ecrimelabs.domain		domain
	ecrimelabs.port	host.port	name
	hannoaxfr.ip	host	name
	hannoaxfr.name		domain
internetcensus2012	item.IP, item.Traceroutes.SourceIP, item.Traceroutes.TracerouteRe-sult.IP, item.ServiceProbes.Result	host	name
	item.Synscans.Ports	host.ports	name
shodan.io	ip_str	host	name
	hostnames, domains		domain
	location.latitude		latitude
	location.longitude		longitude
	title		description
	port	host.port	name
	org	host.organiza-tion	name
	location.area_code, location.city, location.country_code, location.-country_code3, location.country_name, location. dma_code, location.postal_code, lo-cation.region_code		address
	os	host.os	name
	devicetype	host.device_ty pe	name
	cve.cve	cve	name
	cve.description		descr
	cve.date		published-datetime

Название веб-ресурса	Поле по протоколу описания источников для сканирования и извлекаемых данных	Тип сущности	Соответствующее поле типа сущности
maxmind.com	ip_address	host	name
	location_latitude		latitude
	location_longitude		longitude
ripe.net	atlasprobes.probes.address_v4, atlastargets.measurements.dst_addr, dnschain.nameservers, dnschain.-forward_nodes, mlabclients.clients	host	name
	atlasprobes.latitude, mlabclients.-clients		latitude
	atlasprobes.longtitude, mlabclients.-clients		longtitude
	atlasprobes		description
	dnschain.forward_nodes, reversedns.domain		domain
	abusecontacts.holder_info, addressspacehierachy.netname	organization	name
	abusecontacts.emails		contacts
	abusecontacts.morespecific, addressspacehierachy.netname, asroutingconsistancy.prefixes, announcedprefixes.prefixes.prefix, risprefixes.prefixes.v4.originating, risprefixes.prefixes.v4.transitting	subnet	name
	abusecontacts.morespecific, addressspacehierachy.inetnum, asroutingconsistancy.prefixes, announcedprefixes.prefixes.prefix, risprefixes.prefixes.v4.originating, risprefixes.prefixes.v4.transitting		mask
arin.net	net.name	subnet	name
	net.netBlocks.cidrLength		mask
	net.netBlocks.description		description
	org.name	organization	name
	org.city, org.iso3166-1.name, org.streetaddress		address
	poc.emails, poc.phones		contacts
	poc.firstname, poc.lastname	personal	fio
verisign.com	ip	host	name
	domain		domain
premiumdrops.com	ip	host	name
	domain		domain